NEW JERSEY DEPARTMENT OF CHILDREN AND FAMILIES

Policy Manual

Manual:	CSOC	Children's System of Care	Effective Date: 2/16/2018
Volume:	I	CSOC	
Chapter:	G	Privacy and Records	Revised Date: 12/6/2021
Subchapter:	1	Privacy and Records	
Issuance:	3	**Use and Access of CYBER Records by Non-CSOC Employees**	

Purpose:

This issuance establishes policy and procedures pertaining to access to the Children's System of Care's (CSOC) Electronic Behavioral Health Information System, currently known as CYBER, by DCF employees in divisions other than CSOC.

Authority:

- 42 U.S.C. 1301 et. seq.
- 42 C.F.R. 2.1 et seq.
- Administrative Order 6:00, **Confidentiality of Department Information and Records**

Policy:

A) Access to CYBER to be Approved by CSOC

1) DCF employees, other than CSOC or CSOC contracted vendors, shall be permitted to have direct access to CYBER only with the approval of the Assistant Commissioner for CSOC or his/her designee.
2) Access will be granted only to persons with a bona fide need for such access that cannot be met through other means.

3) The Assistant Commissioner for CSOC may designate particular positions within DCF as presumptively requiring CYBER access.
4) A list of currently approved users shall be maintained by CSOC.

B) Monitoring of Approved Users

1) Cost Code Managers or their designees are required to review the roster of users in their cost code that have access to CYBER no less than annually and update the status of users' access with the Assistant Commissioner for CSOC.
2) When a user is no longer with the Department, the user's direct supervisor/manager must immediately submit a CYBER Security Access Form to the NJ SPIRIT Help Desk to deactivate the CYBER user. Within the request, the supervisor shall include the user's name, DCF office, and date of the requested deactivation.
3) Direct supervisors/managers must also immediately notify the NJ SPIRIT Help Desk via the CYBER Security Access Form when users are on or are expected to be on extended leaves of absence (more than 45 days). These accounts will be deactivated at the appropriate time but can be reactivated upon the users return.

C) Provision of CYBER Records for Non-CSOC Purposes

1) CYBER records and information shall be made available to the Division of Child Protection and Permanency (CP&P) and other DCF divisions and staff as permitted by law and for purposes consistent with (D) below.
2) If a youth is open with a Care Management Organization (CMO), CP&P staff shall request information through the youth's care manager. All other requests shall be submitted via email or in writing to the office of the Assistant Commissioner for CSOC.
3) All requests for records and information shall clearly state the purpose for which information is sought.

D) Permissible Use of CYBER Information

1) Protected Health Information (PHI) and protected substance use disorder treatment information obtained from CYBER, directly or indirectly, in print and/or electronic form or through verbal dissemination, may only be used for purposes permitted by the Health Insurance Portability and Accountability Act (HIPAA), 42 CFR Part 2, and other applicable law.
2) All CYBER users are responsible for the protection and safeguarding of PHI from inappropriate use or disclosure. Use of PHI for acceptable purposes include:

a) Investigation of child abuse or neglect allegations, provided that CYBER will not be used as a routine component of the CP&P or SCR screening processes, and only accessed when circumstances indicate that necessary information is or should be found in CYBER.
b) Purposes related to billing and financial reimbursement, including submission of necessary information for Medicaid or other federal reimbursement.
c) Reviews related to the assessment of parental contribution to care.
d) Auditing and performance management activities; or
e) Other purposes permitted by law with the approval of the Director of Legal Affairs.

E) Unauthorized Access or Use of CYBER Records Strictly Prohibited

1) The unauthorized access or use of CYBER records is strictly prohibited.
2) Staff shall not share usernames or passwords, or otherwise facilitate access to the system by persons not authorized to have access.
3) Staff accessing records for any unauthorized purpose do so in violation of HIPAA and other confidentiality laws, as well as the Uniform Ethics Code, and may be subject to disciplinary action up to and including termination.

F) Disputes

1) DCF staff may appeal the denial of CYBER access to the Assistant Commissioner for CSOC or his/her designee. Staff will be notified by the Assistant Commissioner for CSOC or his/her designee of the final decision.

Procedures:

1) Requesting CYBER Access

Requests for CYBER Access shall be made on behalf of an employee by his or her Cost Code Manager or designee, or equivalent, and directed to the Assistant Commissioner for CSOC.

a) Requests shall be made by completing the CYBER Security Access Form for DCF Users and emailing the form to the NJ Spirit Help Desk at njspirithelpdesk@dcf.nj.gov
b) The request will then be forwarded to the Assistant Commissioner for CSOC for approval.
c) Requests cannot be sent directly to CSOC's Contracted System Administrator (CSA),

d) Upon approval, the user will be notified by the NJ SPIRIT Help Desk of their username and password and directions for logging into CYBER.

2) CYBER Deactivations and Lockouts

a) CYBER users will be allowed five login attempts. After five attempts, the user will be locked out and will require a password reset via an emailed password reset process to unlock their account.

b) If a user does not log into CYBER for 90 days, their account will be locked and will necessitate utilizing an emailed password reset process to unlock their account. Once a user successfully logs in, the 90-day timeframe for logins is reset.

c) If a CYBER user is unable to utilize the emailed password reset, the CYBER user must contact the NJ SPIRIT Help Desk at njspirithelpdesk@dcf.nj.gov to unlock their account.

d) If user does not log into CYBER for 180 days, their account will be deactivated. Deactivated accounts can only be reactivated at the request of the Assistant Commissioner for CSOC. A new CYBER Security Access Form must be submitted to the NJ SPIRIT Help Desk at njspirithelpdesk@dcf.nj.gov for consideration of reactivation.

e) The request will then be forwarded to the Assistant Commissioner for CSOC for approval.

f) The complete training guide for CYBER password reset functionality is available on the Contracted System Administrator's website.

3) Appealing the Denial of a Request for CYBER Access

a) DCF staff who wish to appeal the denial of a request for CYBER access may submit a request via email to CSOC.Director@dcf.nj.gov for review to the Assistant Commissioner for CSOC or his/her designee.

b) Such requests shall clearly state

1) the title of the position for which CYBER access is sought,
2) the purpose for which CYBER access is needed, the name and number of the potential user's Cost Code Manager, and
3) the requested duration of CYBER access.

c) The Assistant Commissioner for CSOC or his/her designee shall review the request and communicate a final determination to the requestor.

Key Terms:

- **Contracted System Administrator (CSA)** means the single point of entry for all children, adolescents and young adults (up to age 21) who are in need of

behavioral health, developmental and intellectual disability, or substance use treatment services. PerformCare is the Contracted System Administrator for CSOC.

Forms:

- CSOC-I-G-1-3 ATT1**, CYBER Security Access Form**

Policy History:

- Revised, 12/2021
- Revised, 3/2021
- New policy, 2/2018